REGULATING FOREIGN-BASED INTERNET CONTENT: A JURISDICTIONAL PERSPECTIVE

RICHARD GARNETT*

The recent enactment of the *Broadcasting Services Amendment (Online Services) Act* 1999 (Cth) ("*Online Services Act*") has drawn attention to a significant problem involving the regulation of the Internet; that is, what is the scope of application of national laws[1] in relation to Internet content that is based outside a country but accessible by local residents? This issue has arisen in two distinct contexts. First, where a local resident brings a civil suit arising from the placing of material on a foreign website that infringes his or her rights under the law of the forum country (for example, the content is defamatory or infringes its intellectual property). Second, where content exists on a foreign sourced website or newsgroup accessible in Australia that, if published in this country, would violate local criminal law.

The problem in both cases is that, while such material may infringe Australian law if published or made accessible here, it may be perfectly legitimate content under the law of the place of creation or the law of the country of the host server (if different). An Australian court or legislature would therefore have to balance its interest in protecting its local residents by exercising local jurisdiction over foreign content producers against the need to preserve harmonious relations with foreign countries by not attaching sanction to conduct that is permissible under their laws.

Some writers have described the problem of regulating foreign based Internet content as one of "extraterritoriality"; that is, under what circumstances can a country apply its laws to events outside its geographical boundaries.[2] In one sense, this description is slightly misleading because the Internet is a borderless medium. Conduct on the Internet has effects in every country in which the material is accessible. However, while the technology is universal in nature, national laws have unfortunately remained widely divergent in character, with

* Senior Lecturer in Law, Monash University.

1 Note that this would include State and Territory laws in a federal system.

2 G Smith (ed), *Internet Law and Regulation*, FT Law & Tax (2nd ed, 1997) p 248.

the result that the Internet has dramatically increased the scope for conflict between national legal systems.

Perhaps the best solution to the problem of regulating cross border activity on the Internet would be the creation of an international convention prescribing universally applicable rules. However, given the differences in culture and political and economic systems among countries, particularly in their attitudes to issues such as obscenity and freedom of expression, agreement on the content of universal rules to be applied to Internet transactions may be impossible. Nevertheless, in the less contentious and more uniform area of commercial law, there may be greater incentive to achieve harmonisation.[3]

A more modest proposal to unifying national laws on the Internet may be to conclude an international treaty that provides for a universally applicable 'choice of law rule' in Internet cases. In other words, whenever an Internet dispute arose before a national court involving, for example, content posted on a site outside the country, and the defendant asserted that another country's laws applied, a rule would exist indicating to the national court which law had to be applied. There is currently great debate among private international lawyers as to which system of law should be applied in Internet cases.[4] The range of alternatives proposed includes the place of origin of the offending material, the place of receipt of the material and the place of nationality of the content producer. Interestingly, the CSIRO, in its report on content blocking (commissioned by the Federal Government prior to drafting of the *Online Services Act*), suggested that an international agreement should be concluded identifying the applicable law in Internet cases, with the law of the country of the requesting client to be applied.[5] In the view of this author, however, it is likely to be impossible to lay down a single choice of law rule to govern all Internet transactions, given the array of possible causes of action. Therefore, it may be necessary to adopt a variety of the options referred to above.[6]

However, neither type of convention is likely to be effective in the case of criminal liability because domestic courts do not have the power to enforce foreign criminal laws[7] or apply local criminal law to persons outside the territorial jurisdiction. In order to regulate cross-border Internet crimes, a convention would have to be created that not only identified particular, agreed offences but also provided bases of jurisdiction for national courts to try or extradite offenders.

---

3 The 1996 United Nations Commission on International Trade Law's *Model Law on Electronic Commerce* represents an attempt to harmonise domestic laws in the area of the recognition of digital signatures. Drafted over a three-year period, the Model Law represented the contributions of more than fifty countries, which may augur well for its future implementation.

4 See, generally, J Fawcett and P Torremans, *Intellectual Property and Private International Law*, Clarenden Press (1998) pp 160-1.

5 CSIRO Report, *Blocking Content on the Internet: A Technical Perspective*, June 1998 at 48 (Appendix 5).

6 For example, in the case of defamation, it is arguable that the place of receipt of the information has a strong claim for consideration whereas in the area of copyright, the place of upload may be more appropriate.

7 *Huntington v Attrill* [1893] AC 150.

Hence, it seems that any solution at the international level is unlikely to be imminent, given the contentiousness and complexity of the issues. Until some agreement is reached, however, the current uncertainty in relation to regulating Internet activity will remain.

The other problem with attempting to regulate Internet content offshore is the difficulty of enforcement. If the defendant is the content provider, then it is likely that he or she will be located outside Australia. Suppose an Australian court made orders imposing liability on such a party. Unless a foreign court agrees to enforce such a decree (or in a criminal matter, extradite the accused) the foreign defendant will escape sanction altogether for publication of the offending content. Given that, as noted above, there are significant differences between national laws, particularly in the area of prohibited content, it is very possible that a foreign court may refuse to recognise an Australian decree, particularly if the conduct in question is legitimate under local law.

Thus, it can be seen that both courts and legislatures face serious problems in regulating foreign-based Internet content. Until the enactment of the *Online Services Act*, Australian legislatures had made only a modest attempt to do so. For example, under the laws of Western Australia and the Northern Territory it has been made an offence to use a computer service to "obtain possession" of or "request the transmission" of an article knowing it to be objectionable material.[8] As this legislation is not expressed to apply only to information emanating from within Australia, it would catch an Australian-based recipient of overseas content. However, the obvious limitation of these provisions is that, in imposing liability on the local recipient of the material, they do not attack the problem of the content at its source and, therefore, they fail to prevent the material being accessed in this country. Similarly, in the area of civil jurisdiction, Australian courts have been reluctant to grant relief in respect of offending information on foreign websites. In *Macquarie Bank Ltd v Berg*,[9] the Supreme Court of New South Wales refused to grant an Australian resident an interlocutory injunction to restrain a United States-based defendant from publishing material on a site allegedly defamatory of its reputation under the law of New South Wales. Two reasons were given for this conclusion. First, that there would be difficulty in enforcing an order against a foreign-based defendant; and second, that the effect of such an order would be to restrain publication of the material in any country and so superimpose the law of New South Wales on the world. The concerns of enforcement and jurisdiction mentioned above were therefore paramount.

It was these deficiencies in the regulation of overseas content that led the Federal Government to consider a fresh approach. Given the problems of jurisdiction and enforcement, it was evidently thought neither desirable nor practicable to impose liability on foreign content providers, the originators of the information. Instead, the *Online Services Act* creates a structure whereby the Australian Broadcasting Authority ("ABA"), after receipt of a complaint about a

8 *Censorship Act* 1996 (WA), s 101(1)(b) and (e) and *Classification of Publication and Films Amendment Act* 1995 (NT), s 50Z(1)(b) and (e).

9 Unreported, Supreme Court of NSW, Simpson J, 2 June 1999.

site and having determined that it contained prohibited content, will require an Internet service provider ("ISP") to block content from that source.[10] This obligation placed on ISPs with respect to overseas content is to be contrasted with the duty imposed with respect to material hosted in Australia, which the ABA can request to be removed.[11]

Despite the Government's expressed desire to treat offshore and onshore content equally,[12] it seems that the jurisdictional and enforcement limitations referred to earlier led to the choice of 'blocking' overseas content over the more draconian 'taking down' that is prescribed for local content. Blocking, in all its various forms,[13] would – at its most effective – only have the effect of depriving *Australian* users of access to the material; users in other countries would continue to be able to visit the site. In addition, because the legislation appears to impose a duty only on ISPs based in Australia in relation to overseas content,[14] there is no question of the *Online Services Act* applying to persons outside Australia. Therefore, it seems that the Act is largely inoffensive in terms of its jurisdictional reach.

However, as has been noted by technical experts[15] and senators,[16] while the legislation is jurisdictionally benign, a price may have been paid for this outcome in terms of the effectiveness of the legislation. There is a serious question as to whether content blocking is a technically feasible method of keeping offensive material outside Australia. Further, there is the spectre of adverse consequences for the local e-commerce industry.

It was perhaps in response to these concerns that the ABA, on 16 December 1999, registered a code of practice[17] dealing with the obligations of ISPs in relation to content hosted outside Australia.[18] Under the code, ISPs, instead of having to block content from overseas sites, are now obliged to provide end users with approved content filters.[19] While this approach again raises no jurisdictional issue, its effectiveness in preventing entry of offensive material

---

10 *Broadcasting Services Act* 1992 (Cth), Schedule 5, s 40(1)(c) (as amended by the *Online Services Act*) requires an ISP "to take all reasonable steps to prevent end-users from accessing that source". While the legislation does not mandate a particular technological solution to filtering overseas material, it was generally assumed in the parliamentary debates that content blocking was the method intended. Such blocking may occur at the 'packet' or 'application' levels. See CSIRO Report, note *5 supra*.

11 *Broadcasting Services Act* 1992 (Cth), Schedule 5, s 30 (as amended by the *Online Services Act*).

12 See the comments of Senator Alston, Minister for Communications, Technology and the Arts in Australia, Senate 1999, Debates, vol S8, pp 5220, 5266 and 5422.

13 Note 10 *supra*.

14 Although the terms of the legislation are not explicit on this point, there was no suggestion in the explanatory memorandum that ISPs located outside Australia would be subject to the Act. Note 12 *supra*, pp 3957-3963.

15 CSIRO Report, note *5 supra* at 5-8, 39.

16 See, especially, the Minority Report of Senator Stott-Despoja (Deputy-Leader of the Australian Democrats) in the *Report of the Senate Select Committee on Information Technologies*, December 1998 at 35.

17 Schedule 5, Part 5 of the *Broadcasting Services Act* 1992 (Cth) (as amended by the *Online Services Act*) makes provision for the development of industry codes in relation to certain matters (see s 60). Such a code may be registered by the ABA (s 62).

18 Content Code 2.

19 *Ibid*, cl 6.2.

into Australia appears doubtful, given that the power to access such material remains in the hands of the individual user.

The conclusion to be drawn from the whole debate about regulating foreign-based Internet content, therefore, is that a unilateral national response to the issue is destined to be unsuccessful, given the global and elusive nature of the medium. Either such action leads to jurisdictional disputes with other countries through the application of conflicting national laws, or the measures taken may be technically unworkable, as in the *Online Services Act*. Thus, it is suggested that the conclusion of a multilateral treaty, either to harmonise national laws relating to Internet content or, more realistically, to create a 'choice of law rule' or rules pointing to the applicable national law, may be the only way to achieve effective and enforceable regulation.